Performance Work Statement (PWS)
For
Defense Manpower Data Center (DMDC)
Personnel Security/Assurance (PSA) Systems Support

Contract Vehicle: GSA ALLIANT (Large Business)
Contract Type: Firm Fixed Price

TABLE OF CONTENTS

1.0 Introduction

The Defense Manpower Data Center (DMDC), Personnel Security/Assurance Division (PSA) is seeking experienced professional information technology (IT) services to support its technology governance and customer development, sustainment and operational activities, across the software development life cycles. These services will be performed both onsite DMDC locations and offsite.

2.0 Background

DMDC is part of a Department of Defense (DoD) Field Activity called the Defense Human Resources Activity (DHRA) which supports major programs and initiatives within the DoD. DMDC maintains the central and authoritative store of personnel, manpower, training, and security data for the DoD. DMDC is a geographically separated organization with personnel and facilities located in Alexandria, Virginia; Seaside, California; Boyers, Pennsylvania; Korea; Southwest Asia; and, Germany. While being geographically dispersed, DMDC takes pride in delivering timely, quality support to the DoD and its members. DMDC adds value by ensuring data received from a variety of sources is consistent, accurate, and appropriate when used to respond to inquiries.

DMDC quickly responds to initiatives and informational needs of DoD senior leadership which supports decision-making for a wide variety of organizations. DMDC operates major programs affecting individual members of the DoD, as well as other Federal Departments and Agencies. The programs support Active Duty, Reserve, Guard, and retired military members and their families, as well as civilian and contractor employees of the DoD. These programs include verifying military entitlements and benefits; managing the DoD ID card issuance program; providing identity management for the DoD; helping identify fraud and waste in DoD systems; conducting personnel surveys; performing longitudinal and statistical analyses; developing military selection, classification, and language proficiency tests; and assisting military members and their spouses with quality of life issues and transition to civilian life.

DMDC supports major programs and initiatives within the DoD and maintains the Defense Enrollment Eligibility Reporting System (DEERS), the largest archive of personnel, manpower, training, security and financial data within the DoD. The personnel data holdings, in particular, are broad in scope and date back to the early 1970's, covering all Uniformed Services, all components of the Total Force (Active, Guard, Reserve, and Civilian), and all phases of the personnel life cycle (accessions through separation/retirement). The categories of data archived at DMDC represent significant data holdings and, in most cases, provide the only single source of commonly coded data on the Uniformed Services. These data support decision-making by the Office of the Secretary of Defense for Personnel and Readiness (OUSD (P&R)),

other Office of the Secretary of Defense (OSD) organizations, and a wide variety of customers both within and outside the DoD.

2.1 PSA Systems

On January 15, 2009, the Deputy Secretary of Defense directed that the Department strengthen and refocus the Defense Security Service (DSS) to meet 21st century industrial security and counterintelligence needs. Pursuant to this recommendation, DSS was directed to transfer "DoD enterprise wide IT systems associated with personnel security clearances to the Defense Manpower Data Center." A Memorandum of Agreement between DSS and DMDC was signed on February 2, 2010, which set forth the terms and conditions for the transfer. The transitioned systems included the Defense Central Index of Investigations (DCII); the Joint Personnel Adjudication System (JPAS); improved Investigative Records Repository (iIRR), and the Secure Web Fingerprint Transmission (SWFT). The Defense Information System for Security (DISS), including Case Adjudication Tracking System (CATS) and Joint Verification System (JVS), transitioned to DMDC effective October 1, 2015. These named applications will be known as PSA Applications. The servers for the PSA applications are located at the DMDC in Seaside, CA (iIRR is located in Boyers, PA), and the DISA Data Center in Columbus, OH.

2.1.1 JPAS

JPAS is a repository and centralized processing tool that provides the capability to perform comprehensive personnel security management of all DoD employees, military personnel, civilians and DoD contractors. JPAS consists of two sub-applications:

- The Joint Adjudication Management System (JAMS) - The JAMS sub-application records the eligibility determinations and unclassified investigation comments, supports the adjudication process, and automates security information records. JAMS is a system designed for the Clearance Adjudication Facilities (CAFs).
- The Joint Clearance and Access Verification System (JCAVS) - The JCAVS sub-application enables DoD Security Managers and officers the ability to view current eligibility information. It also provides the ability to update Personnel Security Information and security history.

2.1.2 DCII

DCII is an automated central index that identifies investigations conducted by DoD investigative agencies, and personnel security determinations made by DoD adjudicative authorities. DCII is operated and maintained on behalf of the DoD components and office of the Deputy Under Secretary of Defense for Human Intelligence (HUMINT), Counterintelligence and Security.

Access to DCII is normally limited to the DoD and other federal agencies that have adjudicative, investigative and/or counterintelligence missions.

2.1.3 SWFT

SWFT serves the Defense industry and other DoD users to submit electronic fingerprints (e-fingerprints) for applicants who require an investigation by the Office of Personnel Management (OPM) for a personnel security clearance. Cleared contractors and other DoD users collect and securely transmit e-fingerprints to SWFT for their subsequent release to OPM. The SWFT eliminates the manual paper processing of fingerprints, provides end-to-end accountability for Personally Identifiable Information (PII) data, and expedites the clearance process. SWFT consists of two sub-applications:

- Application for online collection of biometric and biographic data capture and their subsequent integration into electronic fingerprint files. This sub-application is a licensed commercial product.
- Store-and-forward system for collection and distribution of electronic fingerprint files.

This integrated system is also known as SWFT Plus Enrollment or SWFT+.

2.1.4 iIRR

iIRR is a repository for the legacy subject records of any personnel security investigation opened and closed within the DSS' Case Control Management System – Information System (CCMS-IS) prior to its decommissioning on 3 February 2006. Some of the investigative records are stored electronically and some files are on microfiche. The iIRR access is restricted to a team of DMDC staff on a closed network due to the sensitive nature of the investigative records.

2.1.5 Defense Information System for Security (DISS)

In response to the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, the Joint Security and Suitability Reform Team (JRT) identified focus areas to be reformed in order to improve the federal security and suitability clearance process. This new process was outlined by the JRT in the April 2008 Initial Report on Security and Suitability Process Reform, which provided a framework for an enterprise-wide, end-to-end process supported by appropriate IT systems to make hiring, credentialing, and clearance processes meet IRTPA guidelines on efficiency and timeliness.

The Under Secretary of Defense for Intelligence (USD(I)) is the functional sponsor and has established and defined the top level operational requirements for DISS. The DISS solution will support information sharing between various DoD entities, as well as among a number of other federal agencies. It will be managed and maintained by the DISS PMO. The DISS PMO will follow guidance of, and escalate issues to, the appropriate DISS Governance Board. The DISS servers are located at the DoD Consolidated Adjudications Facility (CAF) and Network Enterprise Center (NEC) in additional to DMDC in Seaside, CA and DISA Data Center in Columbus, OH.

DISS will replace various security clearance and suitability systems, enabling consistent standards and reciprocal recognition for all DoD clearances. The DISS program focuses on solutions for three of these reform areas:

- Validate Need – DISS is working with Office of the Director of National Intelligence (ODNI) and OPM to create a federated search capability to support reciprocity and reduce unnecessary duplicate investigation and adjudicative processes.
- Electronic Adjudication (e-Adjudication) – DISS employs technology to apply business rules and render suitability and security adjudication decisions electronically in cases with no actionable issues.
- Continuous Evaluation – Support the Automated Records Check technology so records for existing cleared personnel can be analyzed more often to flag potential concerns.

Enhancing these primary areas of the reform security and suitability processes will allow the DISS program to improve timeliness, reciprocity, quality, and cost efficiencies through the design and implementation of a secure, end-to-end IT solution.

- Case Adjudication Tracking System (CATS) - CATS supports the process of rendering determinations of an applicant's eligibility for clearance and suitability or fitness for employment providing a framework for assessing an applicant's trustworthiness and fitness. To date, CATS is successfully implemented at the Army CAF, Navy CAF, DISCO, Washington Headquarter Services (WHS), and Air Force CAF. These implementations have already achieved substantial improvement in the overall time necessary to adjudicate clearances. CATS is the JPAS JAMS replacement.
- Joint Verification System (JVS) - JVS will provide the functionality for the maintenance and verification of security and suitability information. JVS will support the concept of a virtual Security Management Office (SMO), providing an access point for Security Officers to manage security information, including subject access levels and eligibility. JVS will be JPAS' JCAVS replacement.

3.0 Scope

The Contractor shall provide the full range of IT services, technical and management expertise, and solution-related enabling products in one or more of the functional categories to meet the mission needs of the DMDC. The contractor shall adhere to the performance standards in this contract as well as industry accepted best practices where such does not conflict with the requirements specified while all propose innovative solutions and cost savings initiatives. As identified in individual tasks, information technology solutions/capabilities will support DMDC on a world-wide basis. The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and any other items or resources to perform this scope of work, including non-personal services necessary to deliver sustainment and operational support activities as defined in this Performance Work Statement (PWS) except for where required by the Government as specified in the PWS.

The Contractor shall provide solutions for the following functional and technical categories:

1. Sustainment and Operational Support of PSA Applications
2. Development of DISS Security & Data Services (SDS) and Data Migration
3. Decommission of JPAS (RESERVED)
4. Transition of CATS to DMDC Infrastructure
5. Program Enhancements and Surge Requirements
6. iIRR Production System Stand-up Support
7. Sustainment and Operational Support of CATS
8. Sustainment and Operational Support of JVS
9. ODC in Support for DISS

Services provided under this task order shall include Project Management and Software Development Life Cycle (SDLC) requirements. The specific depth and breadth of the activities will vary over the implementation of the project, and include requirements definition, functional and technical specifications, design, project planning, development, testing, and implementation. With the pace of change, it is impossible to anticipate how IT requirements and programs will evolve over the life of the contracts. These services represent a broad set of contemplated work requirements and must not be construed as the only activities to be to be performed on this task order.

The Contractor will work closely with various divisions within DMDC, DLA personnel, and other agencies to ensure the success of each application. To achieve success the contractor will need to employ a complete understanding of DMDC's system infrastructure, configurations, tools, and components.

4 DESCRIPTION OF REQUIRED TASKS:

4.1 Sustainment and Operational Support of PSA Applications (PSA Apps)

NOTE: For the purposes of this task order, this is an Operations and Maintenance Task. This task shall span the entire period of performance for DCII, iIRR, SWFT, and JPAS. CATS and JVS Sustainment and Operational Support are listed as tasks 4.7 and 4.8.

All PSA applications with the exception of CATS, JVS, and JPAS are fully integrated in the standard DMDC environment. The JPAS application support will be from the Operating System (OS) on up. The SWFT application support will be also from the Operating System (OS) on up, with the exclusion of the data tier. If a task is for a specific application, it will be noted as such.

THE CONTRACTOR SHALL:

4.1.1 Provide ongoing sustainment, operational and production level support for the PSA applications within the production, pre-production, failover, and test environments and ensuring all aspects of the applications, including any reports, continue to function at the efficiency and capability levels intended as detailed in Appendix B "Guidelines and Parameters for Resolving System Problems", and Appendix C "System Outage Notification Procedures". This effort will require support for each of the technologies used for the applications.

4.1.2 Detect all outage/issue/problems that adversely affect the performance and/or vulnerability of the systems and work with DMDC Systems to assist to resolve the outage/issue/problem, and notify the Government/stakeholders, as defined by DMDC, as soon as possible even prior to the resolution in accordance with Appendix B & C.

4.1.2.1 For JPAS, DISS and SWFT: In addition to 4.1.2, the contractor shall have a proactive approach by utilizing automated system-monitoring techniques to identifying recurring problems, reporting to the Government those problems, and recommending solutions to mitigate recurring problems of the same nature. Resolve all outage/issue/problems from the OS level on up. Work with Systems to resolve all outage/issue/problems on the OS level.

4.1.3 Provide support by assisting in identifying and resolving application system problems and/or vulnerabilities. This includes recommendations, consultations, coordination, evaluation, testing and deployment to resolve.

4.1.3.1 For JPAS and DISS: In addition to 4.1.3, the contractor shall identify and resolve application system problems and/or vulnerabilities from the OS level on up.

4.1.4 Provide database administration services that shall perform modifications to the PSA applications while maintaining continuity of the data to include performing schema changes and conversion of the production database during application upgrades and new version releases.

4.1.4.1 For JPAS, DISS and SWFT: This will be administration from the OS on up. For all other PSA applications, this is at the application database level.

4.1.5 For JPAS and DISS: Maintain database replication between all backup site locations and all server replicates.

4.1.6 Support, maintain, and keep the test, development, and pre-production PSA applications consistent with current application upgrades and new version releases, while providing database refreshment of all database instances. Ensure that all data used in these environments follow DMDC's Personal Identifiable Information (PII) Policies. Data will need to be refreshed at the request of the PM or at least once a year.

4.1.7 For JPAS and DISS: Support, maintain, and keep the test, development, and pre-production PSA environment consistent with current application upgrades and new version releases, while providing data refresh on all database instances.

4.1.7.1 For JPAS or DISS: The contractor shall build out the necessary environment(s) in CT to allow for the PII to be removed from Largo and to be used to replace the PII environments that are currently being used by the data team. Some work will be dependent on another contractor.

4.1.8 Assist in failover planning, testing, and execution at least once a year and during any major outage where when the Government deemed failover necessary.

4.1.8.1 For JPAS and DISS: Conduct failover planning, testing, and execution at least once a year and during any major outage when the Government deemed failover necessary.

4.1.9 Modify the applications in accordance with Change Requests (CRs) (**Deliverable 21)** and Problem Reports (PRs) **(Deliverable 22)** approved by the DMDC Technical Point of Contact (TPoC).

4.1.10 Collaborate with PSA system's partnering agencies (e.g., OPM, DSS, Armed Services, Accessions, Industry) to maintain fully functional interfaces, process data; resolve data and/or technical issues; and/or update the interfaces when needed. This includes decommissioning of interfaces when no longer needed and updating the interfaces as the partnering agency transition over to the new ISO country codes, if applicable.

4.1.11 Ensure that quality assurance requirements are enforced for all aspects of the software revision process. This includes collecting and analyzing quality metrics, performing detailed reviews, walkthroughs, requirement traceability analyses, defined verification and validation processes that occur during the course of software maintenance to ensure that requirements are traceable, consistent, complete, and successfully tested. Ensure the software correctly reflects the documented requirements which include conducting, reporting on, and/or participating in formal reviews, informal reviews, inspections, peer reviews, tests, and evaluations to ensure the code meets operational and security requirements and does not negatively impact performance of the system.

4.1.12 Customer, Data and Field Support

4.1.12.1 Maintain and ensure data accuracy and data integrity. Analyze and resolve data errors/issues/problems and resolve. If any data integrity/error/issue with a record is identified, the record shall be updated/corrected within fourteen (14) business days or within timeline specified/agreed upon by the PSA Application PM, and the resolution will be communicated to the Government, stakeholder, customer, and/or interface. If the source of the problem originates from an interface, communication to the data source/interface must be made within 48 hours of discovery to include identification and recommendation to for problem resolution. This coordination with external interface owners/customers for data correction also includes periodic and timely follow-ups until data issue is resolved.

4.1.12.1.1 Due to the current political environment, the level of effort and services originally proposed has significantly increased. This task is to supplement the existing data quality assurance team to ensure data conforms to data standards. This task may include performing quality control checks to JPAS data, verifying scripts, correcting data and ensuring data is meeting standards set by the Government to ensure that JPAS data will not only meet data quality standards but also be able to be migrated from JPAS in the future.

4.1.12.2 Add, create, modify, or delete super users/Non-DOD/special circumstances user accounts or settings within three (3) business days of notification unless immediate add/modification/removal is needed.

4.1.12.3 Create and provide customized reports or data extracts based on DMDC or stakeholder's requirements. Reports or data extracts shall be provided within seven (7) business days from receiving the Government's request or within timeline specified by the PSA Application PM.

4.1.12.3.1 Due to the current political environment and removal of allowing outside agencies the ability to run JPAS reports, there has been a significant increase in the level of effort and reports being delivered by the JPAS team. This task is to supplement the existing team to ensure DMDC is able to meet all reporting requirements.

4.1.12.4 Provide review, evaluation, advice, answers and/or guidance on products or deliverables relating to the PSA Applications to the Government, Stakeholders, Call Center, and customers.

4.1.12.5 For SWFT: Act as the point of contact between the Industry and Government to coordinate and manage day to day SWFT activities. This function is generally known in the SWFT user community as the SWFT Coordinator, and includes the following responsibilities: Monitor and maintain the SWFT mailbox ensuring that all requests, questions, issues and other communications are addressed within two (2) business days; manage and coordinate with OPM the registration and test of fingerprint scanners; coordinate with the SWFT Administrators timely release of electronic fingerprints; coordinate with the Help Desk and the SWFT Administrators the resolution of issues related to the SWFT application; produce and maintain program documentation such as: weekly activity reports, system metrics, SWFT registration documents, and SWFT FAQ's; monitor and analyze processes and procedures related to the SWFT usage, fingerprint submission site and scanning device registration, and make recommendations for improvement and enhancement.

4.1.12.6 For SWFT: The contractor shall act as the point of contact between the online fingerprint enrollment user community and DMDC to manage and coordinate day to day activities. This function includes the following responsibilities: create and manage online enrollment system user accounts; create, manage and assign the enrollment user groups and location profiles; respond to client communications and ensure that all requests, questions, issues and other communications are addressed within two (2) business days; coordinate with the SWFT Coordinator and Administrator timely release of electronic fingerprints; coordinate timely resolution of issues related to online fingerprint enrollment with the Help Desk, SWFT Administrators and technical support; produce and maintain program documentation such as: weekly activity reports, system metrics, and FAQ's specific to online fingerprint enrollment; monitor and analyze processes and procedures related to online fingerprint enrollment subsystem usage, fingerprint submission traffic, site and scanning device registration, and make recommendations for improvement and enhancement.

4.1.13 Testing

4.1.13.1 Develop, conduct thorough testing in the development and test environments to ensure optimum performance is maintained to include functional testing of interfaces and application changes, as defined in the

Functional Test Plan, prior to releasing the software and/or IA patches for testing in the Government's pre-production environment.

4.1.13.1.1 For JPAS and DISS: In addition to 4.1.13.1, upon completion of the contractor's initial testing and quality assurance testing, all software coding will be tested in the Government's pre-production environment to ensure proper validation of enterprise systems and applications prior to deployment into the production environment.

4.1.13.2 Ensure all errors identified during the tests, to include tests in the Government's pre-production environment are resolved. Once testing has been accepted by the Government, the modifications can be deployed to production.

4.1.13.2.1 For DCII; in addition to 4.1.13.1, contractor shall conduct functional testing prior to releasing the software and or IA patches to the production environment.

4.1.14 Configuration Management (CM) Support

4.1.14.1 Perform the CM activities of configuration status accounting, configuration baseline management, creating and maintaining a configuration management library system to control the release of products, manage their history, administering a change management procedure, and tool to track all CRs or PRs to the baseline as well as all issues (problem reports, Deliverable 22)

4.1.14.2 Perform the accepted and practiced DMDC CM processes in conjunction with internal and external procedures, plans, and polices of the Agency to include informing, coordinating, providing and documenting all baseline system documentation, modifications to existing and developing system(s) under the Agency's purview through the DMDC CM group Baseline system documentation includes system designs, build procedures, requirements documents test procedures, problem reports, software code, and system knowledge base.

4.1.15 Information Assurance (IA)

NOTE: For PSA Applications running in standard DMDC infrastructure, the scope of this task will be generally limited to application-level support. For JPAS and DISS, the scope of support is from the OS level on up.

4.1.15.1 Perform all work within the scope of this contract in strict compliance with all applicable DoD Security Regulations and DoD Information Assurance Regulations, USCYBERCOM Orders, Federal Information Security Management Act (FISMA) and DMDC Security policies to include: maintaining the Trusted Facilities Manual and Security Features Users' Guide required by DoD, monthly IA Security Vulnerability Reports, participating in the Certification and Accreditation process, using protective tools such as Security Technical Implantation Guide (STIG), Security Readiness Reviews (SRRs) or checklist on a reoccurring basis using the appropriate tool (or other tool as defined by the Government), providing and implementing the necessary Information Assurance/Computer Network Defense (IA/CND).

4.1.15.2 Create and adhere to procedures & guidelines which are created to comply with DoD and DMDC security policies. Ensure that all data leaving DMDC systems in transit or at rest be protected according to DODI 8500.2. Specific policies are listed as DODD 8500.1; DODI 8500.2; DODD 8570.01-M; DODD-O-8530.1; DODD-O-8530.2; and DoD 8510.10. These policies are available at http://www.dtic.mil/whs/directives/corres/ins1.html.

4.1.15.3 Take immediate action to assess the impact of each vulnerability, develop patching plans, provide First Report requirement, create the necessary Plan of Action and Milestones (POA&M), and test patches to ensure no negative impact. Testing shall be conducted to ensure IAVM actions will not impair system operations.

4.1.15.3.1 For JPAS and DISS In addition to 4.1.15.3, the contractor shall patch all application software and server components accordingly while following DMDC's IA policies and regulations. IAVM compliance will be ensured through 1) the normal Certification and Accreditation (C&A) process, and 2) monthly scanning of the systems using tools used by DMDC. The results of these scans will be sent to the Information Assurance Officer (IAO), to be identified post award.

4.1.15.4 Support obtaining accreditation via certification testing of its respective element(s). This task will consist of process, analysis, coordination, security certification test, self-evaluation, conducting system security assessments, and security documentation support, assisting the Government in the implementation of Certification and Accreditation.

4.1.15.5 Ensure the Information Assurance Manager (IAM) and IAO are informed on system security matters, address specific security issues, and obtain guidance.

4.1.15.5.1 For JPAS and DISS: Provide any necessary documentation (e.g. Certification and Accreditation reports, Monthly Vulnerability Reports, First Reports, POA&Ms) to DMDC's IAO.

4.1.15.6 For JPAS: Proof of Concept has been completed to change EAServer to JBOSS. This task is to complete the conversion process of the JPAS architecture from CORBA to Enterprise Java Beans (EJBs). This entails replacing the EAServer component due to known vulnerabilities and being at end of life, with JBOSS. This includes identifying and resolving potential issues and ensuring that all aspects of the applications, including any reports, continue to function at optimal efficiency and capability levels.

4.1.15.7 For JPAS: JPAS does not have the audit capability to capture all prior associations and access levels for a person category. This task is to capture the person, person category and any associated Organization and SMO affiliation with the start date, separation date, level of access with this association and other relevant data that may be used for audit purposes only.

4.1.15.7.1 For JPAS: JPAS currently receives data requests to remove prior affiliations due to the business rule to only allow one person category. If a user needs the JPAS Team to delete a person category, due to the only one person category business rule and primary key affiliation, the task needs to be able to eliminate the majority of the JPAS Team's data requests by allowing a subject's person category to be updated with the new person category with the correct information as long as it is for the same type of person category and a separated date is associated with the old person category. An example is if a person is no longer affiliated with Navy Reserve and needs a category added for Army Reserve, if the Navy Reserve category is already separated then the interface/user should be able to overlay the Navy category with the Army data. The Navy Reserve Category will be captured in 4.1.15.7 to ensure all associates are captured and can be used for audit purposes.

4.1.16 The Task 1 deliverables (electronic) shall be:

- For All:
    - Project plan/schedule
    - Software Requirements Specifications
    - Release Notes to be distributed to users
    - User Guide – update and deliver if user functionality changes
    - Interface Control Document (ICD) - Update and deliver after interface modification

- For DCII, SWFT, iIRR, and DISS – Test Management Plan (TMP) to be delivered 15 days prior to scheduled test start dates. TMP shall include the following:
    - Functional Test Guide, test plan, test scripts
    - Requirements Traceability Matrix
    - Configuration Management Plan
    - Source code/Configuration files
    - Executable software libraries
    - Low-Level Design Document (Technical Spec)
    - High-Level Design Document (Functional Spec)
- For SWFT:
    - Quarterly Newsletter
- For JPAS and DISS:
    - Administration Guide to include system administration guide, a list of all hardware and software, JPAS requirements, and installation guidelines - Update 30 calendar days prior to end of contract period and deliver to Government

  - Continuity of Operations Plan (COOP) to include Failover and Disaster Recovery Test Plan to include an annual successful failover test and return to production without loss of data - Update 30 calendar days prior to failover test and deliver to Government
  - Interface Control Document (ICD) - Update and deliver after interface modification
  - Weekly Ad Hoc Report
  - Monthly Vulnerability Analysis Report:
    - Vulnerability Scanning and Scanning Report
    - Self-Evaluation Report
  - Monthly IA Report
    - IA/CND Technical Report (to include negative reporting)
    - DIACAP or Risk Management Framework (RMF) Technical Report
    - IA Combined Report
- For DCII specific to the annual RMF process:
  - The following documents:
    - Application Audit Guide
    - Software Development Life Cycle (SDLC)
    - Software Design Documents - Tech & Functional Specs
    - Software Development Plan
    - Threat Model
    - Coding Standards Guide
    - Developer Configuration Management
    - Code Review SOP and checklist
    - Test Plans
    - Vulnerability Test Procedures & Vulnerability test results
    - Vulnerability Analysis
    - Vulnerability Management Plan

4.2 Development of DISS (JVS and CATS)

NOTE: For the purposes of this task order, this is a Research, Development, Test & Evaluation (RDT&E) Task. This task shall span the entire period of performance.

THE CONTRACTOR SHALL:

4.2.1 Complete development of the full set of functional DISS Security & Data Services to include development of data delivery components implementing the functional and technical requirements, architecture, and all data and security services.

4.2.2 Ensure proper authentication and authorization of a user based on their individual role and level are allowed proper access by using subject and security management office (SMO) data services to read data. Authentication will utilize all DOD-approved Public Keys and will utilize existing DMDC application security and operator provisioning services. Please see Appendix I for more information on data definitions (ASIS, EMMA) and how DMDC's security service works.

4.2.3 Develop subject-related data services to create, read, update, and search for subject information.

4.2.4 Develop SMO data services to create, update, and deactivate SMOs, and manage SMO-subject relationship information and tasks.

4.2.5 Develop eligibility data services to create, read, update, and remove eligibility information for subjects.

4.2.6 Develop foreign relationship & foreign trip data services to create, read, update and delete foreign relationship & foreign trip information for subjects.

4.2.7 Develop access data services to grant, remove, suspend, and reinstate access for subjects to classified data.

4.2.8 Develop incident data services to create, update and close incidents that would impact a subject's eligibility and/or access to classified information.

4.2.9 Develop visit data services to create, validate, access, and modify visit information for a subject's visit to a facility to discuss/access classified information.

4.2.10 Develop notification/message data services, including support for continuous evaluation to notify users and SMOs of various activities during the operation of the system.

4.2.11 Ensure, for all services that are developed, full integration with the DMDC Common Update Framework (CUF), Application Programming Interfaces (APIs), DMDC's application security and operator provisioning services, ensuring that proper transactions are maintained at all times, and shall rollback any uncommitted transactions in accordance with ACID.

4.2.12 Ensure that authorized users have the ability to access all functionality of the application to include add, update/modify, delete based upon their user role and level.

4.2.13 Provide systems engineering support to include the development of the software development lifecycle documents and participate in technical reviews of the documents. These including: System Requirements Document (SRD), High-Level Design Document, Low-level Design Document, and System Test Plan.

4.2.14 Complete development of the JVS ETL capability to extract the Oracle JPAS data and transform it into the CUF subject model format and load the data into the DISS JVS database.

4.2.15 Create a new ETL capability to extract person and personnel data from the Oracle JPAS data store and load the data into the DMDC Person Data Repository (PDR).

4.2.16 Create a new ETL capability to extract SMO- and authorization-related data from the Oracle JPAS data store and load the data into DMDC's EMMA data store.

4.2.17 Build an Archive ETL capability to extract the Oracle JPAS data (and DISS JVS Oracle), transform it into an archive format, and load it into the DISS Integrated Data Store (IDS) data warehouse.

4.2.18 Support verification & validation (V&V) activities in collaboration with the Defense Personnel Security Research Center (PERSEREC) as the current custodians of the Data Migration database. Contractor shall work hand-in-hand with PERSEREC staff at DMDC to verify and validate the data migration deliverables.

4.2.19 Develop referential integrity rules to be applied to screened data to ensure that proper relational database design integrity is applied throughout the destination database.

4.2.20 Perform data migration V&V activities on JPAS data over a period of time in order to adequately process the ~9.5 million records. In order to properly execute these activities over an extended period of time, it shall be necessary for Contractor to properly execute V&V scripts using date/time segmentation. Contractor shall inspect and determine whether other segmentation strategies may be necessary to segment data using other data in the JPAS database (e.g. Person, Personnel, etc).

4.2.21 Fully and successfully migrate the existing JPAS data into JVS. This includes ensuring the data is free of data errors, data conversion is complete and accurate, and all identified data errors, inconsistency, and transformations to fix anomalies/data errors are completed. This includes using the existing Sybase-to-Oracle (Vendor) Extract, Transform & Load (ETL) script to transform the data from Sybase to Oracle without changing the structure.

4.2.22 The Task 2 deliverables (electronic) shall be:

- Functional Test Guide inclusive of the test plan, test scripts, requirements traceability matrix to include system, stress, use cases, integration/interface and functional testing to be updated with each release/delivered fifteen (15) business days prior to the scheduled test start date.
- Configuration Management (CM) Plan that follows DMDC CM standards (i.e., Information Technology Infrastructure Library (ITIL)) and applies to the hardware, software (whether acquired or developed), and documentation developed, maintained, or operated by the contractor or DMDC CM. The Configuration Management Plan is due 30 calendar days after task commencement
- Source code and configuration files – all files needed to perform a build of the application into executable format, delivered fifteen (15) business days prior to the scheduled software version test start date
- Executable software libraries – all executable source code, built and bundled together with any and all configuration files needed, in a single deployment payload, delivered fifteen (15) business days prior to the scheduled version test start date
- Project Plan & Schedule, updated and delivered weekly
- High Level Design (HLD) document, Low Level Design (LLD) document, delivered as required upon completion of engineering tasks, not more than 30 calendar days after task completion
- Develop an identity management service for DISS that will allow CATS to add users and retrieve information about existing users through the DoD Identity Management (IdM) system using the CUF.

4.3 Decommission of JAMS (RESERVED)

NOTE: For the purposes of this task order, this is an Operations and Maintenance Task. The Government anticipates task 4.3 to start on (date TBD).

THE CONTRACTOR SHALL:

4.3.1 Decommission of the JAMS applications after CATS (JAMS' replacement) becomes fully-operational. Each application may have its own timeline for decommission of the applications. The contractor shall work with adjudicators to ensure that all adjudications, incidents, and open items are closed. The contractor shall reconcile and migrate JAMS data to CATS. This task also includes decommission of the web applications, databases, and ensuring a user can no longer use the applications. This will be a phased approach. The first phase is to close all open items, resolve any issues, disabling users and/or collaborating agencies the ability to input information into the database. The second phase will be to decommission the application so users can no longer access or input information. A final backup of the JAMS databases will be performed by the contractor. The format of the backup will be determined by DMDC Systems in conjunction with the Program Manager. JAMS will no longer be able to be accessed by users or data providers.

4.4 Transition of CATS to DMDC Infrastructure

NOTE: For the purposes of this task order, this is an Operations and Maintenance Task. The Government anticipates task 4.4 to start on (date TBD).

4.4.1 Transition CATS from the Army infrastructure to a new environment within DMDC's infrastructure that includes DMDC hardware. Prior to the full transition to DMDC's infrastructure, leverage DISS in Army environment as "warm backup" failover location.

4.4.2 Deploy CATS and portal to the new production, pre-production, and disaster recovery site from the Application level up (Commercial off the Shelf (COTS)/Government off the Shelf (GOTS)) within DMDC's infrastructure. The new environment will be located at DMDC in Seaside, CA and DISA Data Center in Columbus, OH.

4.4.3 The objective is to make the environments a fully "warm" standby site (i.e. a site that can failover within 24 hours of failure). This task requires installation planning, support, and installation of the CATS and associated applications, system testing, and application testing. This task also requires the contractor to ensure data replication from production and failover; migrate data, functionality and interfaces to include any coordination with customers/data owners to ensure CATS is fully operational. The contractor shall set up the pre-production environment to be operational and include test data.

4.4.4 Migration to DMDC processes, which includes code check-in; CM processes; Vulnerability Management and the use of DMDC tools similar to JVS. For DMDC software processes, please see "DMDC Application Development Process and PSA Interim Quality Assurance Requirements & Processes" (Appendix Q and Appendix R),

The Task 4 deliverables (electronic) shall be:

- Fully Operational CATS application in DMDC’s production, pre-production and failover infrastructure to include all interfaces, replication and test data
- Disaster Recovery Test Plan
- System Administration Guide - Initial 30 days after award /Updated as required
- Installation Guide Documentation - Initial 30 days after award /Updated as required
- Implementation Plan - Initial 30 days after award /Updated as required
- Hardware/Software Requirements - Initial 30 days after award /Updated as required
- Concept of Operations - Initial 30 days after award /Updated as required

4.5 PROGRAM ENHANCEMENTS AND SURGE REQUREMENTS

4.5.1 The Government anticipates effort could potentially increase as a result of required enhancements typically derived by changes in business processes, agency or regulatory requirements and on-going improvements and upgrades to the current PSA Applications and Infrastructure. For this purpose, the Government reserves the right to increase the estimated ceiling value of this TO by as much as 10% over the life of the TO, if necessary. Such increases shall only apply to additional tasks that clearly fall within the scope of this PWS and within the performance period of the TO, including all available option periods. This task is broken down into two subtasks, and will be tracked separately:

4.5.1.1 Subtask 1: Sustainment and Operations Support

4.5.1.1.1 Additional Support under task 4.1.9

4.5.1.1.1.1 JPAS

4.5.1.1.1.1.1 Update the National Adjudicative Guidelines. This includes adding any new adjudicative guidelines and removing any obsolete. This includes updating tables, addressing any current/historical cases that have the new and obsolete guidelines associated with them

4.5.1.1.1.1.2 Update the Mass Personnel Changes function to prevent a user from obtaining a list of personnel with their SSNs for organizations the user is not in or does not have a relationship to the organization. This should include that the Manage Mass Personnel Change Function will no longer be displayed without a valid Relationship established. The relationship must be on the Person Category record that the user is sign in as. The Person Category Organization search function will not change. If the User selects a Cage Code that he does not have a relationship as the losing and gaining Organization, an error message should be displayed.

4.5.1.1.1.1.3 Enhance Visit functionality to include the following: Add "Additional Information" field to the Add/Modify Visit screen which will allow users to provide the gaining unit security manager with additional and more specific information containing the visit; add Eligibility and Access information for visit information screen, and add access suspended notifications to the visit notification screen.

4.5.1.1.1.1.4 Modify the JPAS Reactivation process be changed to no longer require the Call Center to review/approve the request prior to it going to the Collaborative CAF for implementation. This includes any Reactivate Requests currently in the Call Center/Help Desk queue will be processed accordingly to reassign them to the Collaborative CAF queue. Relevant database updates for these records and notification removal/creation will be handled by a data conversion. It will also include the JCAVS Request to Reactivate a Person Notification will no longer be sent as it was used in the application to inform the Call Center/Help Desk of work that required attention.

4.5.1.1.1.1.5 Remove the Collaborative CAF from the CAF drop down menus on the JCAVS request screens since this CAF does not function like the rest of the CAFs in the drop down menu. The following screens are impacted for JCAVS: Request to Research/Recertify/Upgrade Eligibility (RRU), Incident Report, Interim Sensitive Compartmented Information (SCI)

4.5.1.1.1.1.6 Update the Person Summary header Eligibility Line to be made visible to all JCAVS Users. The JCAVS Person Summary will be enhanced to display the eligibility for all Levels. It is currently only displayed for Levels 7, 8, and 10. Only the eligibility in the JCAVS Person Summary PID section will be modified. This will include all screens that use the JCAVS Person Summary Common PID will be modified. These screens are: JCAVS Person Summary Screen, JCAVS PSP Decision Screen, and JCAVS SOR Update Screen.

4.5.1.1.1.1.7 Modify display the Indoctrination on JCAVS Non-SCI and SCI History Screens. This will include the Indoctrination Date to be displayed as a read-only field on the Non-SCI and SCI Access History screens in the current format. The tutorial and documentation will need to be updated.

4.5.1.1.1.1.8 Modify the OPM data bridge to support HSPD-12 by allowing JPAS users to see the OPM's information regarding HSPD-12.

4.5.1.1.1.1.9 Modify the OPM data bridge that would allow OPM users to add a security incident flag (Yes, No) and to add SMO codes associated with the SMO name on the existing data bridge to OPM.

4.5.1.1.1.1.10 In order to improve user friendliness and the new DMDC look and feel, JPAS needs to update the look and feel of the application. This includes the color scheme, logo, and to make the application more user friendly. This task is limited to color, images, and font.

4.5.1.1.1.1.11 In order to comply with the Privacy Office, JPAS needs to remove the EDI search capability from the Search screen.

4.5.1.1.1.1.12 In order to ensure users have a better JPAS experience, JPAS will need to update the PSM Net Screen to make the SSN an active link to the Person Summary screen for the person. This task is for modifications to the interface. Testing and deployment will occur under normal sustainment activities.

4.5.1.1.1.1.13 JPAS needs to be able to provide the capability for individual users to update their email address, phone number or any other contact information collected by the user profile screen at any time.

4.5.1.1.1.1.14 Modify JPAS to allow tracking for Sigma 14, 15, and 20. Each Sigma will be treated as an Access. The Access can only be indoctrinated by one user group. The Access should only be displayed for 1 year and after a year will be auto debrief. The Access should be displayed on the JCAVS person summary screen in the Access grid. Each Sigma needs to be included in the interfaces as an existing access.

4.5.1.1.1.1.15 AFPC is migrating their MILPDS data interface feed from Direct:Connect to Secure File Transfer Protocol (sFTP), which will align the AFPC with other agencies' JPAS interface. AFPC interface shall be updated to generate flat flies that will be processed by PID Queue and will require the two-digit state/country code changed to two separate fields. JPAS inbound/outbound interface will exchange MILPDS data via flat files standard through sFTP Server.

4.5.1.1.1.1.16 Scattered Castles interface shall be updated to allow JPAS to send an incident flag ("Y" (Yes) indicator value for open Incident and a "N" (No) value for no open incidents), updated eligibilities, and polygraph dates. All values will be sent to Scattered Castles (SC) in both the full or partial loads. To prevent conflict between JPAS and SC interface; SC must modify their side of the interface to process the new incident flag and polygraph dates.

4.5.1.1.1.1.17 The DEERS interface shall be updated to submit requests for all 31 birth days each month even when the month has less than 31 days. For example, in February, the requests for birth days on the 29th, 30th and 31st are currently not sent to DEERS.

4.5.1.1.1.1.18 The contractor shall convert the DQI Account Removal script (DQI 71692) to be a systematic function of JPAS. This would remove JPAS accounts after 45 days to be in compliance with IA.

4.5.1.1.1.1.19 The contractor shall add the ability to lock (view/modify) a person of interest (POI) JPAS record to prevent unauthorized look-ups. If a POI is looked up, the user will see an error message stating that the record is unavailable for view.

4.5.1.1.1.1.20 The contractor shall modify the application to not allow invalid DOBs to be submitting to the application. The DOB range is to allow a record to be submitted with the age being from 16 years of age to 85 years of age. If a user is updating JPAS with an invalid DOB, an error message will be given and the user will have the ability to update the DOB prior to saving in the application.

4.5.1.1.1.1.21 The contractor shall update the CATS interface to be a bi-directional web service that would allow JPAS to send incident information to CATS and CATS to send data to JPAS. The CATS to JPAS data will consist of all the existing data, incident information, new HSPD-12 eligibilities, and to correct the current erroneous investigation date issue.

4.5.1.1.1.1.22 The contractor shall add the audit capability to the SII-clearance Bridge. JPAS needs to be able to identify who has viewed JPAS data from this bridge and have it stored in our audit tables.

4.5.1.1.1.1.23 The contractor shall update the JPAS so when a separation date is put on a subject’s record, the PID Source is changed to JPAS instead of leaving it at its existing PID Source.

4.5.1.1.1.1.24 The contractor shall ensure when a new eligibility and investigation is on a person’s record that the subject’s eligibility an d investigation on the top of the JPAS Person Summary Screen is the same as the eligibility in adjudication history and investigation history. The eligibility and investigation should not be based on hierarchy.

4.5.1.1.1.1.25 The contractor shall update the existing CE interface to be a bi-directional web service that would allow CE to receive a Full Data on an as-needed basis, transactional data on a daily basis and allow CE users to click on a hyperlink to see real-time single subject JPAS data. In addition, JPAS will need to be able to accept incident information from CE and write and display the incident information in JPAS.

4.5.1.1.1.1.26 The contractor shall create a web service that would work with an outside application to provide a green/red light status that would confirm a person’s eligibility/access based on a matrix.

4.5.1.1.1.1.27 The contractor shall update the ISFD Interface to process Industry KMP File and remove KMP from the Category Classification Table in JPAS. This would prevent KMPs from being created in the JPAS application when they are not on the ISFD KMP file. This would also allow the ISFD file to create a KMP person category in JPAS with an associated Organization.

4.5.1.1.1.1.28 The contractor shall create a flag within the Person information to indicate whether or not a JPAS subject had a SIGMA access ever. This is a Y/N Sigma flag that can be under the Exceptions flag.

4.5.1.1.1.1.29 ~~The contractor shall create a new JPAS SCI Access code (ARK) that will allow only JCAVS Level 2 and 3 users to indoctrinate or debrief SCI access. JCAVS Level 4-10 users will be able to see a Yes or NO indicator for SCI access as well as deactivate the existing SCI access code, HSL.~~

4.5.1.1.1.1.30 The contractor shall modify JPAS to allow a JCAVS user to add an Industry Person Category to a subject (regardless of Person status) without having to be in the same SMO that added the person or a SMO that has a relationship with any non-DOD Person Category.

4.5.1.1.1.1.31 The contractor shall update JPAS to provide an e-QIP “Click to Sign (CTS)” function allowing signature attachments to be uploaded directly to OPM for non-Accession requests. The Add/Modify Investigation Request screen shall disable the View Signature pages once signed in e-QIP.

4.5.1.1.1.1.32 The contractor shall add a new method to the Accessions web service to enable all the OPM statuses for an investigation request to be returned to the submitter. This new method can be used by all Services and it will not cause any problems for the Services if they do not want to use it.

4.5.1.1.1.1.33 The contractor shall update the Automated Continuing Evaluation System (ACES) web service that will allow only Persons with an active Person Category to be returned. If inactive person, respond with an error message.

4.5.1.1.1.1.34 The contractor shall update JPAS systems (JAMS and JCAVS) to prevent all levels of JPAS Users’ from accessing and viewing their own records in JPAS Select Person Screen and allow an error message to notify the users of their misuse of JPAS.

4.5.1.1.1.1.35 The contractor shall ensure sufficient resource(s) are added to the contract to meet the current needs of the data reporting and clean-up. Historically, JPAS data reporting and clean-up has not been as high as it has recently been due to the Washington Navy Yard Shooting. By adding additional resource(s), this should allow the contractor to meet the current business requirements.

4.5.1.1.1.1.36 The contractor shall modify JPAS to treat the subject as a non-DOD person once all of their DOD Categories have been separated or archived and being reactivated.

4.5.1.1.1.1.37 The contractor shall expand the remove user stored procedure to additionally remove all JPAS accounts (JCAVS, JAMS, Super User) if not logged in successfully in the last 45 days.

4.5.1.1.1.1.38 The contractor shall implement Tier 3 and 3R Investigation/Case Types in JPAS. They will replace the NACLC and ANACI investigation types.

4.5.1.1.1.1.39 ~~The contractor shall build out the necessary environment(s) in CT to allow for the PII to be removed from Largo and to be used to replace the PII environments that are currently being used by the data team. Some work will be dependent on another contractor.~~

4.5.1.1.1.1.40 The contractor shall update the JPAS application and e-QIP interface to support the addition of a 14-digit e-QIP PIN. This PIN will be used by the applicant to access e-QIP. On the JPAS side, the application will have to be updated to pass the PIN to the applicant. OPM will update their WSDL to add the PIN. The PIN will only be submitted back to the requester.

4.5.1.1.1.1.41 The contractor shall update CE incident web service to include person status code.

4.5.1.1.1.1.42 The contractor shall implement the Tier I, II, IV, and V investigation types into JPAS to be align with current policy.

4.5.1.1.1.1.43

4.1.1.1.1.1 SWFT

4.1.1.1.1.1.1 Modify SWFT to accept the 5 DOD Approved Public Key credentials at a medium token to medium hardware compliance in accordance to DOD regulations. This solution should be similarly to the previously developed JPAS PK-enabling solution and allow users with valid certificates to logon to SWFT. The contractor will utilize to the maximum feasible extend the code that has been developed by Salient. This includes the capability to self-register non-CACs and associate the token with a user account. This should be implemented using a phased approached allowing SWFT user to logon using a PK token or username/password. The first phase should be implemented around November 30, 2013. The second phase would be to eliminate the username/password capability which should be implemented in March 2014.

4.1.1.1.1.1.2 Modify SWFT with the capability to perform a File Import from External Locations. The solution will provide the utility for periodic automatic import of e-fingerprint files from one or more external locations (e.g., one or more directories residing on a server that is external to the SWFT system.) Must be completed by Sep 30, 2013.

4.1.1.1.1.1.3 Provide the capability to preview all OPM Required Fields in the e-fingerprint file. All required fields for e-fingerprints going to OPM shall be validated. If a required element is missing or is in incorrect format, the solution will display a question mark in the e-fingerprint preview window of the SWFT web application. In the SWFT Administrator console, all required fields and values, except fingerprint images, shall be made viewable in the Preview window.

4.1.1.1.1.1.4 Provide for a new 'Site Manager' Administrator Role. This role will facilitate the management of user accounts that are associated with one or more specific Cage Codes. Site Manager accounts will be created and managed by an administrative role currently known as the Industry Account Manager. More than one Site Manager accounts can be created and managed by a single Industry Account Manager. Executive Administrators will also be able to manage the Site Manager accounts.

4.1.1.1.1.1.5 Provide for the assignment of a Multi-Company Role to Companies. A company must be granted Multiple Company Upload permissions (via the company Create/Edit screen). This solution will add a Multi-Company Role option to the Add Company and Edit Company screens. Only when a company has this capability granted/enabled, then the Multi-Company Role can be assigned by account administrators to user accounts of that company. If a company does not have this capability granted/enabled, then the Multi-Company Role cannot be assigned to the company users.

4.1.1.1.1.1.6 Provide for a management of Multi-Company Uploader role by the Industry Account Managers. The solution will allow the SWFT administrators, currently known as the Industry Account Managers and site managers to grant the Multiple Company Uploader role to regular SWFT users. The current capability of the Executive Administrators to assign the Multi-Company Uploader role will be preserved.

4.1.1.1.1.1.7 Provide the capability to assign one or more scanners to a Site. This solution will give the SWFT administrators the ability and utility to manage fingerprint scanners similar to the way they currently can with the SWFT user accounts.

4.1.1.1.1.1.8 Modify SWFT to deactivate any user account after 90 days of inactivity. This solution should lock users after 30, put them on inactive status at 60, and deactivate after 90.

4.1.1.1.1.1.9 Allow for the Prevention of Duplicate TCN Prefixes. This solution will prevent entering a duplicate TCN prefix in the SWFT online scanner registration form. This solution will provide the capability to reject duplicate TCN prefix during the scanner registration. Must be completed by Sep 30, 2013

4.1.1.1.1.1.10 Add SON/SOI/OPAC Codes to the BiometricInformation Table and the OPAC codes to the BiometricArchive table and applicable reports. Provide the capability to allow these codes to be configured in the Test TAB in the SWFT Administration Console for acceptable value combinations. Must be completed by Sep 30, 2013

4.1.1.1.1.1.11 Provide the capability to Auto-Resize Web Pages to Fit within the Browser Window. This solution will automatically resize the SWFT web pages to fill the entire browser window, and eliminate any unused white space at the bottom of all SWFT web pages.

4.1.1.1.1.1.12 Allow for Processing of .SUB Files. This solution will expand the list of selectable file extensions to include .sub files. This will expand the options for fingerprint file uploads to include file name extensions other than .EFT, namely the files with file name extension .SUB.

4.1.1.1.1.1.13 Develop a configurable utility that will copy EFT submissions from the BiometricInformation Table to the BiometricArchive Table based on multiple SON/SOI/OPAC criteria. Modify the BiometricArchive service to utilize the SON/SOI/OPAC criteria for sending the EFT submissions to the external Biometric Collection Archive.

4.1.1.1.1.1.14 Integrate the DOD eFP Pilot infrastructure into a new environment within DMDC's infrastructure that includes DMDC hardware. The new environment will be located at DMDC in Seaside, CA. This task requires installation planning, installation, and support of the DOD eFP Pilot hardware and software components, system testing, and application testing. The DOD eFP Pilot system must be ready for production by January

31, 2014. Decommission the DOD eFP Pilot system after the pilot production period ends.

4.1.1.1.1.1.15 The contractor shall modify SWFT to provide PK-enabled log on for users of Secure Web Fingerprint Enrollment (SWFE), which is a new subsystem that is being added to SWFT. The SWFE consists of BioSP (server component) and WebEnroll (web application component), both are products licensed from Aware. The solution must and allow access to SWFE only to users with appropriate permissions.

4.1.1.1.1.1.16 The contractor shall provide a new 'Enroller' user role to SWFT. This role will allow access to SWFE, a subsystem of SWFT. This role will be managed by administrative roles that already exist in SWFT. The solution will include the update of the SWFT user administration interface and reports.

4.1.1.1.1.1.17 The contractor shall modify the SWFT capability of EFT file import from external locations by associating each external file location to a source identifier, such as CAGE Code or Organization Code. The solution will allow SWFT users, whose account is associated with such CAGE /Organization Code to run the same reports as are currently provided for files submitted to SWFT via web interface. Implement the solution in form of up to 200 file locations residing both on servers within the DMDC internal production network and servers running in DMZ.

4.1.1.1.1.1.18 The contractor shall provide and implement the SWFT capability to operate in a load balanced environment. The solution must support concurrent operation of at least three SWFT application servers and three BioSP servers, and at least two data tier servers running in a physical cluster.

4.1.1.1.1.1.19 The contractor shall provide a search utility for quick location of a company, organization, site, scanning device records and fingerprint transactions. Each search result must provide a link to screen allowing data update if applicable and appropriate.

4.1.1.1.1.1.20 The contractor shall modify SWFT screens and reports to eliminate display of PII data where not needed or appropriate; to group and sort results in accordance with established user preference; to make reports exportable in formats compatible with MS Office 2010 and higher.

4.1.1.1.1.1.21 The contractor shall modify the SWFT CRI management utility to allow deletion of unneeded entries.

4.1.1.1.1.1.22 The contractor shall provide an intuitive user interface for management of scanning devices.

4.1.1.1.1.1.23 The contractor shall modify SWFT so that VPN tunnel for outgoing transactions is not closed during transmissions.

4.1.1.1.1.1.24 The contractor shall provide a 'Transfer to Archive' option for EFTs in the Hold for Archive Tab.

4.1.1.1.1.1.25 The contractor shall modify SWFT to auto-generate email notification to users when status of their scanning device has changed.

4.1.1.1.1.1.26 The contractor shall modify SWFT to auto-generate email notification to users whose account is to be suspended within certain number of days. The number of days for the advanced email notification must be configurable.

4.1.1.1.1.1.27 The contractor shall provide a configurable capability for real-time verification that an incoming EFT was generated on a scanner workstation that has been registered and approved in SWFT.

4.1.1.1.1.1.28 The contractor shall install and configure SWFT in development and test infrastructure provided by DMDC.

4.1.1.1.1.1.29 The contractor shall integrate the BioSP infrastructure with SWFT in a new load balanced environment within the DMDC infrastructure that includes DMDC hardware. The new environment is located at DMDC in Seaside, CA and Columbus, OH. The Seaside location contains a test and production environment. This task requires installation planning, installation, configuration and support of the BioSP software components and their future releases and patches, system testing, and application testing in an integrated SWFT/BioSP system. The BioSP software and documentation will be provided by a third party vendor.

4.1.1.1.1.1.30 The contractor shall revise the SWFT application to support sending EFTs to one or more destinations determined by the EBTS CRI or TCN value in the EFT. The destinations will be identified by one or more email addresses, and the release of the EFTs will occur with or without a specified timeframe. EFTs that do not match any predetermined criteria will be assigned an interim status that will make them available for a review by SWFT administrators, and manually releasable to any destination. The contractor shall apply the solution to all existing EFT destinations and add FBI as a new destination.

4.1.1.1.1.1.31 ~~The contractor shall modify SWFT to encrypt each EFT file record stored in SWFT system, using encryption method and algorithm that is compliant with current US Government and DOD standards applicable to protection of Personally Identifiable Information (PII) data.~~

4.1.1.1.1.1.32 The contractor shall modify SWFT to provide a replicable SWFT web service for secure EFT file transfer from an application that is external to SWFT. As a minimum, the web service will receive EFT files, confirm the success or failure of each file transaction to the sending application, and make the file available for SWFT processing.

4.1.1.1.1.1.33 The Contractor shall modify SWFT to add a utility for real-time monitoring and reporting the user sessions and their assignment to servers, execution status of distinct fingerprint transactions (e.g., the count of backlogged transactions awaiting the receive, release, or other processes), and task table information (e.g., last run, parameters, and other data items).

4.1.1.1.1.2 DCII

4.1.1.1.1.2.1 Implement an Age-Out Report Display and Export, which will enable DCII users to select the number of records reported and displayed on the web page. The choice shall include 20, 50, 100, and 500 records per page. The report will be made exportable in XLS, HTML, PDF, and comma-separated list format.

4.1.1.1.1.2.2 Implement Multiple Formats in Phone Number Input Fields, which will allow input of phone numbers in several acceptable formats such as (XXX)XXX-XXXX; (XXX) XXX-XXXX; XXX-XXX-XXXX; XXX.XXX.XXXX. The solution will extract all digits from the user's input, and then format them into the current standard DCII format XXX-XXX-XXXX for 10-digit phone numbers, or XXX-XXXX for 7-digit phone numbers. All other numbers will be displayed as concatenated digits without any separators. All phone numbers will be saved in the database as displayed after being reformatted.

4.1.1.1.1.2.3 Implement a Left/Right Trim of Text Input, which will trim space characters from both ends of an input string (excluding file numbers). Trimmed input value will be stored in the database.

4.1.1.1.1.2.4 Provide the capability to log into the DCII web application with one of the 5 DOD Approved Public Key credentials. The solution shall include the capability to self-register a non-CAC token, and associate the token with a user account. The solution must support a user with a single token, but having multiple levels of DCII permissions (e.g., regular User, Agency Administrator, Executive Administrator). The solution shall provide a temporary option to use either user ID and password, or PIV-compliant PKI token to log into DCII during the transition from logID-password logon to PK-enabled logon. The contractor will utilize to the maximum feasible extend the concepts and code that has been previously developed for PK-enabling the JPAS and SWFT. Must be completed by 03/31/14.

4.1.1.1.1.2.5 The contractor shall update DCII to use ISO-3 Country Codes for the batch file, the user interface and the database. This needs to include allowing batch users to submit a FIPS 140 or ISO-2 and convert the batch data into the ISO-3 country code value before storing it in the database.

4.1.1.1.1.2.6 The contractor shall create a web service from bi-directional DCII to CATS that would allow DCII data to be viewed in the CATS application and to allow CATS users to make a record request without logging into DCII. Audit information will need to be captured on CATS users making the record request.

4.1.1.1.1.2.7 The contractor shall provide support for standing up a new DCII Contractor Test/Pre-production environment by uploading data from the test environment to the newly created databases. They shall establish, maintain, and keep the Contractor Test/Pre-production application consistent with current upgrades and new version releases, by providing database refreshment of all database instances. They shall complete successful stress testing, assist with batch user testing and PIV card testing in the Pre-Production environment ensuring application functionality and interfaces are fully operational before deployment to Production, with no loss or corruption of data. All data used in this environment follows required Personal Identifiable Information (PII) Policies.

4.1.1.1.1.3 DCII/iIRR Reconciliation

4.1.1.1.1.3.1 Reconcile the DCII and iIRR systems to sync the background investigation records utilizing the DCII and iIRR batch processes already in place by means of the following steps in listed order:

4.1.1.1.1.3.2 Identify discrepant data between the DCII and iIRR systems.

4.1.1.1.1.3.3 Implement a process allowing for changes (purges) in iIRR to be synchronized with the DCII system.

4.1.1.1.1.3.4 Implement a process for the DCII Beyond Retention/Age Out report to be transmitted and loaded into the iIRR system.

4.1.1.1.1.4 ~~iIRR~~

4.1.1.1.1.4.1 ~~Modify iIRR to accept the DOD Approved Public Key credentials in accordance to DOD regulations. Modification will be applied to the iIRR application in the DMDC Seaside environments. Solution should be similar to the previously developed JPAS PK-enabling solution, except AS-IS should be used instead of the F5 since all iIRR users are CAC holders. Create User~~

~~Management screens to allow for username/password to be used only to register CACs. This task should be implemented by 03/31/14.~~

4.1.1.1.1.4.2 ~~The contractor shall remove PKI enabled authentication from iIRR 5.1 and replace with User Name/Password authentication via LDAP.~~

4.1.1.1.1.4.3 ~~The contractor shall alter data transmission protocol on web services for application presentation from HTTPS to HTTP.~~

4.1.1.1.1.4.4 ~~The contractor shall configure LDAP and newest iIRR version.~~

4.1.1.1.2 Additional support under task 4.1.10

4.1.1.1.2.1 Modify the JPAS Accession's interface that would allow SSBI/PR check in JPAS that runs at the same time JPAS is querying for the NACLC. If the accession service submits a NACLC request and the applicant has a completed SSBI investigation within the last 10 years then JPAS would return an NIR001. The accession service could then submit the request again specifying a break in service when there is a service break of 2 years or greater. This change will be applies to all Accession Interface. The investigation types of SSBI, SBPR and PPR will be used. An error message should be displayed with the reason and investigation closed date. It will include text indicating to resubmit with the break in service indicator if needed. This task is for modifications to the interface. Testing and deployment will occur under normal sustainment activities.

4.1.1.1.2.2 Modify the DCPDS interface to update organization and sub-agency data in JPAS. The data will be provided from DCPDS through the ORG file. The data will be loaded into the Organization table. This task is for modifications to the interface. Testing and deployment will occur under normal sustainment activities.

4.1.1.1.2.3 RESERVED

4.1.1.1.2.4 Establish a one-way batch interface from JPAS to the Army Central Contracts Security Portal (ACCS). The data contained in this interface will be the SCI Access information on cleared Army-owned contractors working for the Army SMO W4VYAA in XML format. These data elements for Access Suspension, Action by Service SMO (SCI only for Indoctrination/debrief), Eligibility Change (Name, Eligibility, Eligibility date and SSN, Incident Update (SSN, Name, Incident date, Status for Industry only), Message from CAF (CAF Response only into notes), and Separation with accesses (Name, SSN, Organization, Status, Date and Access). Application, reports, or other interfaces will not be affected. A transactional data file will be provided on the JPAS FTP server to be picked up by the Army on a weekly basis. A seed data file will be provided initially then only on a scheduled quarterly basis (if needed) to ensure all data is synchronized. This task needs to be completed to deployment by March 2014. This interface was established under a previous task order. The interface needs to be revised to remove data elements from the interface for deployment.

4.1.1.1.2.5 Due to the current political environment, JPAS needs to modify the JPAS NSA Interface. The following CRs will need to be implemented: CR 1974 that does not allow NSA to create duplicate records. This will allow NSA to update Access in JPAS; CR 1975 that allows NSA to update the Removed By edit on the Person Category records submitted through the NSA interface to allow the record to be processed if there are no SMO Person Category records for the person. Currently, the record is rejected when the Removed By field is populated but there are no SMO Person Category records for the person. This allows NSA Records to be processed if there are no SMO Person Category records and the Removed By Date is populated; CR 2106 which stops Adjudication Case lines from being generated by the OPM interface for NSA and Issue 37047 corrects the duplicate removal of non-Industry person categories. The NSA interface will be modified to be parameter driven to indicate which agency is using the code. Also, unused code from the current NSA interface will be removed to improve the maintainability of the interface. This task is for modifications to the interface. Testing and deployment will occur under normal sustainment activities.

4.1.1.1.2.6 Due to the current political environment, JPAS needs to modify the JPAS Scattered Castle interface as requested by NSA. The modification of the Scattered Castle interface will allow all identified eligibilities be sent to Scattered Castles to include but not limited to denial, revoked and suspended. This task is for modifications to the interface. Testing and deployment will occur under normal sustainment activities.

4.1.1.1.3 Additional support under task 4.1.12

4.1.1.1.3.1 For JPAS: Rewrite all JPAS' reports in the identified new reporting tool that will be used for all JPAS reports. The tool will need to go through DMDC's new software process that includes testing and installation of the software in the various environments. Convert all of the identified/consolidated JPAS' reports. This will include the programming and initial testing. This will include not only the reports in the JPAS application used in JAMS and JCAVS, the Management Ad Hoc reports, but also the Statisticians reports. The rewrite of the JPAS reports from Cognos to the new tool should capture a complete reporting capability for JPAS' JAMS and JCAVS users. Finalize testing and deployment will occur under normal sustainment activities.

4.1.1.1.3.2 DISS: DISS must be able to receive data from CE in order to place a new investigation on a subject's record. This will include a CE Alert Flag to identify if a CE alert is on a subject's record as well as a CE investigation history start date and end date on a subject's record. There may be multiple CE investigations, dependent on DoD affiliation. There also may be multiple CE alert flags at various times.

4.1.1.2 Subtask 2: Development Support (Optional)

4.1.1.2.1 At award the value of this task will be $0. If work needs to be accomplished under task 4.5, a modification will be issued to exercise the optional task and incorporate the additional work into the task order. The maximum value of this task cannot exceed 10% of the original awarded value of this contract.

4.1.1.2.2 Individual actions will be in incorporated by contract modification in accordance with the Program Enhancements and Surge Requirements found in Section 4.5 of the PWS.

4.1.1.2.3 Anticipated projects include:

- Modification of applications due to policy changes
- Addition of interfaces
- SWFT user enrollment and registration of scanning devices in support of OUSD(I) deadline for transition to electronic fingerprint submission by Dec 31, 2013
- DCII migration to PK-enabled log in
- Integrate the User Deactivation Utility into the DCII application
- Remove the SSNs from the directory paths in the iIRR Production Towers

4.1.1.2.4 DISS Tiger Team Analysis (OPTIONAL)

The contractor shall provide a professional 'tiger team' and conduct a review of the Defense Information System for Security (DISS) system for a 4-week effort. Specifically, the review will focus on DISS's ability to meet performance objectives and anticipated service level agreements (SLA). As a result of the fact that the DISS architecture was inherited by DMDC from another organization there were a number of issues that did not surface until the initial deployment of the first DoD component occurred, which was on 31 March 2017. The

DISS Tiger Team Analysis is a preventative effort to ensure that unanticipated issues do not occur during future deployments of DISS. The Government anticipates and expects that an experienced team outside of the current DISS team will perform this review. A report of findings is a required deliverable. (See 7.0, Deliverables and Reports, below.)

4.6 iIRR Production System Stand-up Support and Isolated Environment Application Modifications

NOTE: For the purposes of this task order, this is an Operations and Maintenance Task. The Government anticipates task 4.6 to start on (date TBD) and be completed by date TBD).

THE CONTRACTOR SHALL:

4.6.1 Provide support for the preparation, planning, and execution of the rebuild of the iIRR Production application and database at DMDC Boyers in an isolated operational environment. Provide support to the DMDC Systems Division's Government and contractor personnel by helping them understand the application configurations and requirements.

4.6.2 Ensure the modified Production system operates within DMDC Boyers' isolated environment. The Contractor shall be responsible for sustainment tasks including defect fixes, defect tracking, delivery of fixes, application code modifications to support hardware, configuration, and/or network changes, updates to guides and design documentation.

4.6.3 Provide full Production Support for future releases and deployments to include delivery and configuration of application, configuration of Weblogic parameters, configuration of LDAP schema and user groups, configuration of additional dependent COTS software.

4.7 Sustainment and Operational Support of CATS

NOTE: For the purposes of this task order, this is an Operations and Maintenance Task.

4.7.1 The contractor shall perform all tasks, and provide all deliverables described in task 4.1 for the sustainment and operational support of CATS and portal.

4.8 Sustainment and Operational Support of JVS

NOTE: For the purposes of this task order, this is an Operations and Maintenance Task.

4.8.1 The contractor shall perform all tasks, and provide all deliverables described in task 4.1 for the sustainment and operational support of JVS.

4.9 Other Direct Costs (ODCs) in Support of DISS

The Government may require the Contractor to incur ODCs resultant to performance under this task order. Such requirements shall be identified prior to or at the time of award and/or may be identified during the course of performance, by the Government or the Contractor. Reimbursement shall be as a cost re-imbursement and made as specified in the task order invoicing requirements.

Non-Travel ODC items having a total procurement cost over $3,000 shall have the written approval of the Client Representative and the GSA COTR. Federal contracting laws and regulations apply to all Contractor open market purchases of materials and equipment under this task. Prices must be determined fair and reasonable from competitive sources and are subject to Government audit. The Contractor shall maintain records documenting competitive sourcing, in strict compliance with the competition requirements set forth in the Federal Acquisition Regulation (FAR), for all material and ODC purchases. The Contractor shall provide copies of all such documentation upon request from the Government to verify that the Contractor complied with the competition requirements set forth in the FAR. No profit or fee shall be allowed on ODC costs.

All ODC items purchased by the Contractor for the use or ownership of the Federal Government shall become property of the Federal Government. If the Contractor acquires hardware/software maintenance support for performance and support under this task order, all licenses and/or contractual rights to receive title shall be turned over to the Government. The Government's liability to reimburse the Contractor for costs incurred from the acquisition of hardware/software maintenance support shall be limited to costs incurred during the period of the order for which the Government received the said hardware/software maintenance support acquired by the Contractor on a cost reimbursable basis.

The cost reimbursable not-to-exceed ODCs limit is established for each performance period of the task order (RFP Attachment A – Pricing Template). It is noted that the ODC amounts are estimates and the Government reserves the right to increase or decrease this estimate during performance as necessary to meet requirements. Any ODC requirements that arise in excess of the limitations set forth above shall be incorporated through a modification to this task order.

Prior to procurement of any ODCs, the Contractor shall coordinate with and receive in writing all the necessary specifications/descriptions and authorizations from the Government.

5.0 Period of Performance

The base period of performance for this task order shall be a one (1) 6-month base period from the date of award with three (3) 1-month option periods that will be exercised at the discretion of the Government. The Contractor shall be given written notice 15 days prior to the end of any period on the intent exercise.

The period of performance is expected to begin on September 16, 2016.

6.0 Place of Performance

The primary work location will be at the contractor's location(s) with some DISS Development personnel in Seaside, CA. Possible travel to the following DMDC locations: DoD Center in Seaside, CA; Mark Center in Alexandria, VA ; Iron Mountain in Boyers, PA ; DISA Data Center in Columbus, OH.

7.0 Deliverables and Reports

The contractor shall provide the deliverables and reports shown in the table below.

Item	PWS Ref	Title	Distribution	E	H	Initial Due Date	Subsequent Due Date
Overall							
Deliverable 1	RFP Attachment C	Non-Disclosure Agreement	COR		1	Signed statements are due, from each employee assigned, *prior to* performing *ANY* work on this task.	
*Deliverable 2	7.3	Senior Management Reviews (SMR) Report	COR CO TPOC GCOR CS	1 1 1 1	1	NLT 45 DACA	NLT 15th of each month
Deliverable 3	10.1	Transition Plan – Incoming Transition	COR TPOC	1 1	1	Due 5 DA Project kickoff meeting	Final due 5 DA receipt of COR comments
Deliverable 4	10.1	Transition Plan – Outgoing Transition	COR TPOC	1 1	1	Due 90 days prior to Task Order expiration, or when requested by the COR	Updated as required

Deliverable 5	7.5	Quality Control Plan	COR TOA	1 1	1	Due 10 DA Project kickoff meeting	Final due 15 DA receipt of COR comments or 45 DA award
TASK 1							
*Deliverable 6	4.1.16	Program Management Plan and Schedule	COR AM TOA	1 1 1	1 0	Due 5 DA Project kickoff meeting	Final due 15 DA receipt of COR comments
Deliverable 7	4.1.16	Software requirements specification	COR	1		Due 45 DACA	Updated upon request
Deliverable 8	4.1.16	Release notes	COR TPOC	1 1		Due NLT 10 Days prior to any software update/release	Final due 5 DA receipt of COR comments
Deliverable 9	4.1.16	User Guides	COR TPOC	1 1	0 1	Due NLT 10 prior to change in user functionality	Updated upon request
Deliverable 10	4.1.16	Interface Control Document (ICD)	COR TPOC	1 1		Due 10 DA interface modification	Final Due 5 DA COR and TPOC comment receipt
Deliverable 11(DCII, SWFT, iIRR, and DISS)	4.1.16	Test Management Plan (TMP)	COR TPOC CO GCOR	1 1 1 1	1 1	Due 15 Day prior to scheduled testing	Final Due 10 DA after COR and TPOC comments
Deliverable 14	4.1.16	SWFT Quarterly Newsletter	COR TPOC	1 1		Due 100 DACA	Every Quarter
Deliverable 15 (For JPAS and DISS)	4.1.16	Administration Guide	COR TPOC	1 1		Due 45 DACA	Due 30 days prior to Task Order expiration, or when requested by the COR
Deliverable 16 (For JPAS and DISS)	4.1.16	Continuity of Operations Plan (COOP)	COR TPOC AM			Due 45 DACA	Update Due 30 calendar days prior to failover test and deliver to Government

Deliverable 17 (For JPAS and DISS)	4.1.16	Interface Control Document (ICD)	COR TPOC			Due 10 DA interface modification	Update as needed
Deliverable 18 (For JPAS)	4.1.16	JPAS Weekly Report	COR TPOC			15 DACA	Weekly, NLT the 2nd business day
Deliverable 19 (For JPAS and DISS)	4.1.16	Monthly Vulnerability Analysis Report	COR TPOC			NLT 45 DACA-	NLT 15th of each month
Deliverable 20 (For JPAS and DISS)	4.1.16	IA Report	COR TPOC			NLT 45 DACA-	NLT 15th of each month
Deliverable 21	4.1.9	Change Requests	COR TPOC	1 1	1	30 DACA	Updated as required
Deliverable 22	4.1.9	Problem Reports	COR TPOC	1 1	1	30 DACA	Updated as required
TASK 2							
Deliverable 23	4.2.22	Functional Test Guide	COR TPOC			Due 15 days prior to testing	Due 5 DA COR and TPOC comments
Deliverable 24	4.2.22	Program Management Plan and Schedule	COR AM TOA	1 1 1	10	Due 5 DA Project kickoff meeting	Final due 15 DA receipt of COR comments
Deliverable 25	4.2.22	Configuration Management (CM) Plan	COR TPOC AM	1 1 1		Due 30 DACA	Final due 5 DA COR comments
Deliverable 26	4.2.22	Source code and configuration files	COR TPOC AM	1 1		(15) Business days prior to the scheduled software version test start date	Updated as needed

Deliverable 27	4.2.22	Executable software libraries	COR TPOC			(15) Business days prior to the scheduled software version test start date	Updated as needed
*Deliverable 28	4.2.22	Project Plan & Schedule	COR TPOC GCOR CO			Due 5 DA Project kickoff meeting	Final due 15 DA receipt of COR comments
Deliverable 29	4.2.22	High Level Design (HLD) document, Low Level Design (LLD) document	COR			As required	Final due 30 DA completion of TASK 2
TASK 5 **Subtask 2**							
Deliverable 30	**4.1.1.2.4**	**4.1.1.2.4 DISS Tiger Team Analysis Report**	**tbd**			**tbd**	**tbd**

- *these deliverables shall be submitted for formal acceptance within the GSA ITSS procurement system.
- All deliverable due dates are in calendar days unless otherwise noted.
- If an optional task is exercised, the deliverables table will be updated to incorporate the deliverables for the respective systems and time frames.

Abbreviation	Definition
AM	Acquisition Manager
GCOR	GSA Contracting Officers Technical Representative
COR	DMDC 1Contracting Officer's Representative for the Task order
CS	Contract Specialist
CO	Contracting Officer
TPOC	DMDC Technical Point of Contact
DA	Days after
DACA	Days after contract award (award of this order)
DAEOM	Days after the end of the month
Days	Calendar Days unless otherwise specified

DID	Data Item Description
E	Electronic Copy
H	Hard Copy
NLT	Not Later Than
PWS Ref	Performance Work Statement Reference (paragraph number)
TOA	Task Order Administrator

7.2 Problem Reports

Notify the DMDC COR, GSA COTR and GSA CO of any problems or potential problems affecting performance. Verbal reports of problems shall be followed up with written reports.

7.3 Senior Management Reviews (SMR)

Participate in SMR Reports (see Appendix E for acceptable sample format). An SMR report shall be submitted every 15th of each month. The monthly SMR report shall summarize the following information:

- accomplishments during the period,
- problems met or anticipated,
- activities anticipated during the next reporting period,

These reports shall be submitted to the Contracting Officer's Representative (COR) by e-mail and in GSA ITSS system. Each monthly SMR report shall be submitted by the 15th business day of the month following the period reported upon.

7.4 N/A

7.5 Quality Control Plan

Produce a Quality Control Plan (QCP) which will be used as the contractor's internal plan to insure delivery of quality products and services under the terms of the contract. The QCP shall detail the contractor's internal controls for services under this contract and shall have a direct relationship to the proposed terms of the Performance Requirements Summary (PRS), see Appendix A. The outline for the QCP shall be submitted ten (10) days after project "kickoff" meeting. The completed QCP shall be delivered forty-five (45) calendar days after award.

7.6 Delivery, Inspection, and Acceptance Instructions

Deliver all end items specified in this PWS / Deliverable table electronically (with contractor's letterhead - cover letter) to the COR, TPOC, and CO unless otherwise specified. The

Government will review any 'draft' documents and notify the contractor of approval or recommended changes to be made in the 'final' version within thirty (30) business days. 'Final' deliverables are then due within ten (10) business days after receipt of any Government comments on the draft unless otherwise specified by the Government.

7.7 Meetings

Participate in the initial "kick off" meeting: This meeting shall be conducted within the first ten (10) business days after contract award.

Participate in bi-monthly status meeting: The purpose of this meeting is for coordination and information sharing with other DMDC. This meeting should contain all initiative statuses (e.g. status, timelines, risks, issues, etc.), open DMDC/stakeholder's ad hoc reports, recommendations, and any other necessary information that the Government needs to be aware of.

The deliverable (electronic and hard copy) shall be the following:

- Provide meeting minutes to DMDC COR within five (5) business days

8.0 Contractor Personnel

8.1 Key Personnel Requirements

The following labor categories are considered key personnel by the Government:

- Program Manager
- Senior Systems Engineer
- Database Administrator/Manager
- Senior Test Engineer

A key person is someone who is integral and indispensable in completing this task order. Key personnel shall be available at project start. The Government requires that at least one Key Personnel be identified as the primary point of contact for this task order. The contractor shall comply with applicable provisions of the ALLIANT GWAC regarding key personnel and personnel substitutions. Additionally, the contractor shall comply with the following:

a. The contractor shall notify the COTR and DMDC COR at least ten (10) calendar days before making changes in task personnel.
b. The contractor shall provide a replacement resume to the COTR and DMDC COR at the time of notification. Personnel shall be of equal or superior qualifications as the individual being replaced.
c. The resume must be approved by the Government prior to assignment of the

replacement personnel to this task order.

One person on the contractor staff shall be the Task Order Manager, a key personnel, and be the Government's technical point of contact for this task order.

8.2 Identification of Contractor Employees

All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. Electronic mail signature blocks shall identify contractor/company affiliation. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed. Contractor personnel occupying collocated space in a Government facility shall identify their workspace are with their name and company/contractor affiliation.

8.3 Organizational Conflict of Interest

Contractor and subcontractor personnel performing work under this contract may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.), or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

8.4 Unauthorized Disclosure

The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases. If either the Government or the Contractor discovers new or unanticipated threats or hazards, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

9.0 Security

9.1 The Contractor and all Contractor personnel with access to or responsibility for nonpublic Government data under this contract shall comply with DoD Directive 8500.1 Information Assurance (IA), DoD Instruction 8500.2 Information Assurance (IA) Implementation, DoD Directive 5400.11 DoD Privacy Program, DoD 6025.18-R DoD Health Information Privacy Regulation, DoD 5200.2-R Personnel Security Program, and Homeland Security Presidential Directive (HSPD) 12.

9.2 The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data. At a minimum, this must include compliance with DoD 8500.1 and DoDI 8500.2 and provisions for personnel security and the protection of sensitive information, including Personally Identifiable Information (PII).

9.3 Contractor systems and information networks that receive, transmit, store, or process nonpublic government data must be accredited according to the Certification and Accreditation process and comply with annual Federal Information Security Management Act (FISMA) security control testing. All systems subject to the Certification and Accreditation process must present evidence of Certification and Accreditation (C&A) testing in the form System Identification Profile (SIP), Certification and Accreditation Implementation Plan, Certification and Accreditation Scorecard, and Plan of Action and Milestones (POA&M). Evidence of FISMA compliance must be presented in the form of a POA&M. The Contractor will be responsible for the cost of IA C&A and FISMA testing required for any Contractor owned and operated network, facility and/or application processing DoD information.

9.4 The Contractor shall ensure all media containing sensitive information (e.g., hard drives, removable disk drives, CDs, DVDs) considered for disposal will be destroyed. Prior to destruction, media will be sanitized, i.e., all prudent and necessary measures shall be taken to ensure data cannot be retrieved through known conventional or unconventional means.

9.5 Prior to beginning work on this contract, all Contractor personnel with access to or responsibility for nonpublic Government data under this contract must comply with DODI 5200.2-R and the Contractor shall ensure that all such personnel are designated as no less than an IT-II or equivalent.

9.6 Contractor personnel with access to DoD nonpublic Government data must comply with HSPD-12 Personal Identity Verification (PIV) issuance requirements, known as the Common Access Card (CAC) for DMDC and must:

a. Be CAC or PIV ready prior to reporting for work. At minimum all Contractor personnel must obtain/maintain a favorable FBI National Criminal History Check (fingerprint check), two forms of identity proofed identification (I-9 document), and submit a National Agency Check and Law Credit (NACLAC) vetting package for processing. Obtaining CAC or PIV ready status is the responsibility of the contracting agency. It is the responsibility of the contracting agency to notify DMDC when this is complete.
b. Be citizens of the United States.
c. Maintain favorable FBI National Criminal History checks and ensure completion and successful adjudication of a NACLAC as required for Federal employment.

9.7 If at any time, any Contractor person requiring a CAC is unable to obtain/maintain an adjudicated NACLAC, the Contractor shall immediately notify the DMDC Information Assurance Branch (IA) remove such person from work under this contract.

9.8 To the extent that the work under this contract requires the Contractor to have access to DoD sensitive information the Contractor shall after receipt thereof, treat such information as confidential and safeguard such information from unauthorized use and disclosure. The Contractor agrees not to appropriate such information for its own use or to disclose such information to third parties unless specifically authorized by the Government in writing.

9.9 The Contractor shall allow access only to those employees who need the sensitive information to perform services under this contract and agrees that sensitive information shall be used solely for the purpose of performing services under this contract. The Contractor shall ensure that its employees will not discuss, divulge or disclose any such sensitive information to any person or entity except those persons within the Contractor’s organization directly concerned with the performance of the contract.

9.10 Contractor shall administer a monitoring process to ensure compliance with DoD Privacy Programs. Any discrepancies or issues should be discussed immediately with the Contracting Officer Representative (COR) and corrective actions will be implemented immediately.

9.11 The Contractor shall report immediately to the DMDC CIO / Privacy Office and secondly to the COR discovery of any Privacy breach. Protected PII is an individual’s first name or first initial and last name in combination with any one or more of the following data elements including, but not limited to: social security number; biometrics; date and place of birth; mother’s maiden name; criminal, medical and financial records; educational transcripts, etc.

9.12 Government may terminate this contract for default if Contractor or an employee of the Contractor fails to comply with the provisions of this clause. The Government may also exercise any other rights and remedies provided by law or this contract, including criminal and civil penalties.

9.13 The Contractor shall be responsible for safeguarding all government equipment, information and property provided for Contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

9.14 JPAS and DISS require two personnel with Top Secret/Sensitive Compartmented Information (TS/SCI). One in production support and one in data analysis.

9.15 JPAS and DISS require personnel to have a favorably adjudicated Single Scope Background Investigation (SSBI), with either Secret or Top Secret access level.

9.16 DCII and iIRR require personnel to have a favorably adjudicated Single Scope Background Investigation (SSBI), with either Secret or Top Secret access level only if the personnel need to access production data; otherwise a Secret clearance is required.

9.17 SWFT requires personnel to have a Secret clearance.

9.18 Government Facility Access - For selected personnel at contract award and in coordination with Technical Point of Contact (TPoC) the contractor shall request and obtain Common Access Cards (CAC) for logical and/or physical access to Government resources. The Contracting Officer's Representative (COR) shall notify the contractor of any increased security requirements, if they occur, and the contractor shall submit adequate clearance packages within 10 calendar days of identification of increased security requirements.

10.0 OTHER PERFORMANCE REQUIREMENTS

10.1 Orientation Briefing

Within two weeks of award, the Contractor shall conduct an orientation briefing for the Government, inclusive of DMDC and GSA personnel. The Government does not want an elaborate orientation briefing nor does it expect the Contractor to expend significant resources in preparation for this briefing. The intent of the briefing is to initiate the communication process between the Government and Contractor by introducing key task participants and explaining their roles, reviewing communication ground rules, and assuring a common understanding of subtask requirements and objectives. The Orientation Briefing's place, date and time shall be mutually agreed upon by both parties within a week from the date of award. The completion of this briefing will result in the following:

a) Introduction of both Contractor and Government personnel performing work under this Task Order.

b) The Contractor will demonstrate confirmation of their understanding of the work to be accomplished under this PWS.

The Contractor shall provide two (2) hard copies of their proposal (technical and price) to the Government at award.

Transition Plan

The contractor shall develop an outgoing transition plan (Deliverable 4) to provide a detailed transition strategy/plan from their own support to another contractor. The outgoing transition plan shall be due 90 days prior to task order completion.

The transition plan~~s~~ at a minimum shall include: participating in the planning and transition of the applications during the period of performance; provide a communication plan which details the transition plans and schedule with all stakeholders; provide detailed briefings regarding the structure of the database tables, software required continuing maintenance, and operation of systems developed under this contract; transfer all project materials (source code, documentations, etc.) to the successor Contractor upon direction from the Contracting Officer and in a manner prescribed by the Government. The transfer shall be completed by the expiration date of the contract and shall include provision by the incumbent Contractor of accurate and complete data files and pertinent documentation.

10.3 Hours of Operation

The contractor is responsible for conducting business, between the hours of 8 a.m. to 5 p.m., Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons.

Contractor operations support personnel shall provide pro-active monitoring of the Personnel Security and Assurance (PSA) applications and the COTS products that support them with the DMDC enclave during normal business hours (0800 to 1700 hours EST/DST, Monday to Friday). The contractor shall also have personnel available for on-call after-hours emergency support either through VPN or on-site, twenty-four hours a day, seven days a week. It is anticipated that the PSA systems will be instrumented with enterprise management and monitoring tools (e.g. BMC patrol) that can automatically alert contractor operations support personnel (via email or pager) in case of system problems.

10.4 Government Holidays

The following Government holidays are normally observed by Government personnel: New Year's Day, Martin Luther King's Birthday, Presidential Inauguration Day (metropolitan DC area only), President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, Christmas Day, and any other day designated by Federal Statute, Executive Order, and/or Presidential Proclamation. Or any other kind of administrative leave such as acts of God, (i.e. hurricanes, snow storms, tornadoes, etc.) Presidential funerals, or any other unexpected Government closures.

10.5 Contractor Interfaces

The Contractor and/or its subcontractors may be required as part of the performance of this effort to work with other Contractors working for the Government. Such other Contractors shall not direct this Contractor and/or their subcontractors in any manner. Also, this Contractor and/or their subcontractors shall not direct the work of other Contractors in any manner. The Government shall establish an initial contact between the Contractor and other Contractors and shall participate in an initial meeting. Any Contracting Officer's Technical Representatives (COTR) of other efforts shall be included in an initial meeting.

10.6 Remote Access

Contractor will use DMDC's remote access network infrastructure. The contractor will furnish:

- Stable, high-quality Internet Bandwidth
- Non-GFE workstations capable of installing and executing hardware and software necessary to use VPN remote access tools for network authentication and access control points. Non-GFE workstations shall include standard peripheral devices required for complete functionality (i.e., monitor, keyboard, mouse, etc.). In addition, the contractor shall provide the following additional peripheral devices: Common Access Card (smartcard) compatible card reader.
- The contractor shall comply with all information technology security requirements. For Non-GFE workstations capable of access the DMDC network, the contractor shall maintain patch levels in compliance with the DoD's IAVA program; maintain antivirus updates; and, maintain DMDC mandated software configurations.
- The contractor shall, when security incidents are detected regardless of the source of the incident, promptly notify the DMDC help desk as well as immediately discontinuing the use of workstations. If malware is the source of the security incident, the contractor shall promptly eradicate the malware.
- Non-secure Telephone, facsimile, and voicemail capabilities.

The Government shall provide VPN remote access tools as GFE. Non-GFE workstations shall be capable of installing and executing the following software configurations (VPN access tools): Cisco VPN client; Microsoft Windows Terminal Service client; ActivClient 6 or newer; and Antivirus DoD approved vendor & version.

Remote access is controlled via a Common Access Card (CAC)-enabled to access Virtual Private Network (VPN). The contractor shall ensure that only those personnel having a compelling operational need will request such access and shall keep this number to the absolute minimum necessary to accomplish the mission. This access will be granted to personnel only via an approved System Access Request (SAR). Access will only be granted from the contractor's or DMDC's network.. This subnet will conform to DoD Directive 8500.1, DoD Instruction 8500.2, and appropriate Security Technical Implementation Guides, including, but not limited to, Secure Remote Computing, Enclave Security, and Network Infrastructure. The subnet will require accreditation by the DMDC Designated Accrediting Authority (DAA) under the Certification and Accreditation Process. The contractor shall assist with the implementation of the Certification and Accreditation on this subnet.

11.0 TASK ORDER ADMINISTRATIVE MATTERS

11.1 Travel

Travel may be required at irregular intervals to the DMDC locations listed in section 6.0. The Contractor will be reimbursed for travel to provide support at a Government site or other site as may be specified and approved by the COR under this effort. All travel shall be approved, by the COR, prior to commencement of travel. The contractor shall be reimbursed for actual allowable, allocable, and reasonable travel costs, including local travel, incurred during performance of this effort in accordance with the Joint Travel Regulations (JTR) currently in effect on the date of travel.

The task order will establish a ceiling of $30,000.00 each year which cannot be exceeded without the advance approval of the contracting officer. No profit or fee shall be added.

11.2 Government Furnished Property/Information

The contractor shall assume it will be responsible for providing all resources including all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items necessary to provide the non-personal services detailed herein at the contractor facility. The contractor's environment does not have to mirror the production, pre-production, and failover environments.

NOTE: Development and Contractor Test environments (to include software, hardware, and licenses to support these environments) WILL NOT be provided by DMDC under this task order for JPAS and SWFT. Environments provided for JPAS and SWFT are pre-production, production, failover, and other replicated environments used for reporting.

The only exception is the Government will provide the DISS contractors working on-site at the DMDC Data Center in Seaside, CA with GFP for use (i.e. computer, cubicle, chair, telephone, etc.)

11.3 Payment Information

The Period of Performance (POP) for each invoice *shall* be for one calendar month. The contractor *shall* submit only one invoice per month per order/contract. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

(1) The end of the invoiced month *(for services)* or

(2) The end of the month in which the products *(commodities)* or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Labor Hour and Time and Material orders/contracts each invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It *shall* also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, *as well as* the grand total of all costs incurred and invoiced.

For Labor Hour and Time and Material orders/contracts each invoice *shall clearly indicate* both the current invoice's monthly "burn rate" and the total average monthly "burn rate".

The contractor *shall submit* all required documentation (unless exempted by the contract or order) as follows:

For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.

For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

Note: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

Note: For Firm Fixed Price, Labor Hour, and Time and Material fiscal task items:

Charges:

- All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.
- For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

Credits:

- If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.
- When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance **SHALL NOT** be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number and the period to which the credit pertains. The contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration
Finance Division
P.O. Box 71365
Philadelphia, PA 19176-1365

Posting Acceptance Documents: Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS to allow the client and GSA COR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The receiving agency has the following option in accepting and certifying services:

a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services.

Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services. The contractor shall seek acceptance and electronically post the acceptance document in GSA's electronic Web-based Order Processing System, currently ITSS. After acceptance of the invoice by the CR, the Contractor shall submit a proper invoice to GSA Finance (*www.finance.gsa.gov/defaultexternal.asp*) not later than five (5) workdays after acceptance by the Government of the product, service, and/or cost item.

Note: The acceptance of the authorized agency customer representative is REQUIRED prior to the approval of payment for any invoiced submitted and shall be obtained prior to the approval of payment. In order to expedite payment, it is *strongly recommended* that the contractor continue to include the receiving agency's electronic acceptance of all the services or products delivered, with signature of the authorized agency customer representative and the date of acceptance, as part of the submission documentation.

Note: If *any* invoice is received without the required documentation and, the customer's electronic acceptance, the invoice *shall* be rejected in whole or in part as determined by the Government.

Posting Invoice Documents: Contractors shall submit invoices to GSA Finance for payment, after acceptance has been processed in GSA's electronic Web-Based Order Processing System, currently ITSS. The contractor is to post the invoice on GSA's Ft. Worth web site, *www.finance.gsa.gov/defaultexternal.asp*

Content of Invoice: The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1. GSA Task Order Number
2. Task Order ACT Number
3. Remittance Address
4. Period of Performance for Billing Period
5. Point of Contact and Phone Number
6. Invoice Amount
7. Skill Level Name and Associated Skill Level Number
8. Actual Hours Worked During the Billing Period
9. Travel Itemized by Individual and Trip (if applicable)

10. Training Itemized by Individual and Purpose (if applicable)
11. Support Items Itemized by Specific Item and Amount (if applicable)

Final Invoice: Invoices for final payment must be so identified and submitted within 60 days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA COR before payment is processed, *if necessary*.

Close-out Procedures.

General: The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

11.4 Correspondence

To promote timely and effective administration, correspondence shall be subject to the following procedures:

a) Technical correspondence (where technical issues relating to compliance with the requirements herein) shall be addressed to the Contracting Officer's Representative (COR) with an information copy to the Contracting Officer (CO) and the Contract Administrator (CA).
b) All other correspondence, including invoices, (that which proposes or otherwise involves waivers, deviations or modifications to the requirements, terms or conditions of this PWS) shall be addressed to the Contracting Officer with an information copy to the COTR.

11.5 Points of Contact

Contracting Officer Representative (COR)
(b) (6)
Defense Manpower Data Center (DMDC)
4800 Mark Center Dr.
Alexandria, VA 22350

(b) (6)

GSA COR / Information Technology Manager
Michael Baumann
IT Specialist, GSA FAS R3
215-446-5852
Michael.baumann@gsa.gov

GSA Contracting Officer
Christine Chaapel
Contracting Officer, GSA FAS R3
Voice (215) 446-5857
Fax: (215) 814-6164
christine.chaapel@gsa.gov

12.0 CLAUSES

FAR 52.217-8	Option to Extend Services (Nov 1999) – and/or –
FAR 52.217-9	Option to Extend the Term of the Contract (Mar 2000)
FAR 52.224-2	Privacy Act (Apr 1984)
FAR 52.239-1	Privacy or Security Safeguards (Aug 1996)
FAR 52.222-54	Employment Eligibility Verification (Jan 2009)
FAR 52.227-14	Rights in Data
FAR 52.227.16	Additional Data Requirements (Jun 1987)
FAR 52.232-18	Availability of Funds
FAR 52.237-3	Continuity of Services (Jan 1991)
FAR 52.224-1	Privacy Act Notification (Apr 1984)
FAR 52.204-9	Personal Identity Verification of Contractor Personnel
FAR 52.245-1	Government Property
FAR 52.223-2	Affirmative Procurement of Biobased Products Under Service and Construction Contracts (Jul 2012)
FAR 52.246-4	Inspection of Services- Fixed Priced (Aug 1996)
FAR 9.5	Organizational Conflict of Interest
252.209-7999	REPRESENTATION BY CORPORATIONS REGARDING AN UNPAID DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW (DEVIATION 2012-00004) (JAN 2012)

13.0 Section 508 Compliance requirements

The contractor shall support the Government in its compliance with Section 508 through-out the development and implementation of the work to be performed. Section 508 of the

Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities who are members of the public seeking information or services from the Federal Agency, have access to and use of information and data that is comparable to that provided to the pubic who are not individuals with disabilities, unless an undue burden would be imposed on the agency. The Offer shall review the following websites for additional 508 compliance information.

http://www.section508.gov/index.cfm?FuseAction=Content&id=12
http://www.access-board.gov/508.htm
http://www.w3.org/WAI/Resources

14.0 APPENDICES

Appendix A – Combined Performance Requirements Summary
Appendix B – Guidelines & Parameters for Resolving Systems Problems
Appendix C – System Outage Notification Procedures
Appendix D – Quality Control Plan (QCP)
Appendix E – Senior Management Review (SMR) Template
Appendix F – JPAS Technical Information
Appendix G – DCII Architecture
Appendix H – SWFT Technical Information
Appendix I – EMMA Functional Specifications v4.1
Appendix J – SecurityInfrastructureService_5.0_FunctSpec
Appendix K – Common Update Framework for Developers
Appendix L – CUF Data Access Processors
Appendix M – CUF Subject Processors
Appendix N – N/A
Appendix O – iIRR Production Environment
Appendix P – Quality Assurance Surveillance Plan
Appendix Q – DMDC Application and Development Process
Appendix R – PSA Interim Quality Assurance Requirements & Processes
Appendix S – Historical PSA Systems Information